

UNITED STATES DISTRICT COURT

for the
District of Delaware

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Case No. 23-252M

a Chromebook laptop (S/N: 7L0w242); Teclast laptop (S/N: a Chromebook laptop (S/N: 7L0w242); Teclast laptop (S/N: 8353S212663404); Acer laptop (S/N: NXEFUEG00302108EA92N00); HP PC computer (S/N: 4CE1151FG7); PC Tower Eraser Mediom MT39 computer (S/N: 162207050900275); Dark blue Galaxy S6 cell phone; Dark blue Samsung cell phone in red/black case; Dark blue Samsung cell phone with no case; and External hard drive

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the _____ District of _____ Delaware _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 875(c), 2261A(2), 641, 1343, and 1957	Threats Made in Foreign Commerce, Cyberstalking, Theft Concerning Programs Receiving Federal Funds, Wire Fraud, and Money Laundering

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Katherine Martinez

Applicant's signature

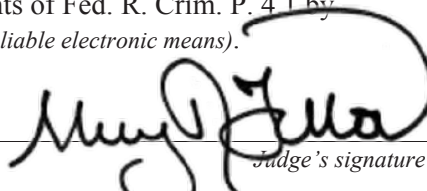
Katherine Martinez, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____
 telephone _____ *(specify reliable electronic means).*

Date: June 5, 2023

City and state: Wilmington, DE


Judge's signature

Sherry R. Fallon, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

IN THE MATTER OF THE SEARCH OF A
CHROMEBOOK LAPTOP(S/N: 7L0w242),
TECLAST LAPTOP(S/N: 8353S212663404) ,
ACER LAPTOP(S/N:
NXEFUEG00302108EA92N00), HP PC
COMPUTER(S/N: 4CE1151FG7), A PC
TOWER ERAZER MEDIOM MT39
COMPUTER (S/N: 162207050900275), A
DARK BLUE GALAXY S6 CELL PHONE,
A DARK BLUE SAMSUNG CELL PHONE
IN RED/BLACK CASE, A DARK BLUE
SAMSUNG CELL PHONE WITH NO CASE,
AND AN EXTERNAL HARD DRIVE
CURRENTLY LOCATED IN AN
EVIDENCE LOCKER AT THE FBI
WILMINGTON RESIDENT OFFICE

Case No. 23-

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Katherine Martinez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—nine electronic Devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. Your Affiant has been a Special Agent with the FBI since July 7, 2019. As part of my duties, I investigate violations of federal law, including bank fraud, complex financial crimes, money laundering, wire and mail fraud, and thefts from government programs. I have gained experience in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have also participated in

investigations involving transnational criminal enterprises engaged in money laundering. I have been trained in the execution of financial search warrants resulting in the seizure of financial documents and United States Currency. I have personally participated in the execution of seizure of United States Currency resulting from fraudulently obtained Covid-19 pandemic related government loans. Prior to my employment as a Special Agent with the FBI, I worked as an Assistant District Attorney in Philadelphia, Pennsylvania, from November 2014 to July 2018, where I reviewed dozens of search warrants and arrest warrants for approval prior to submission to the local magistrate and advised local law enforcement on investigative methods and legal issues. As an Assistant District Attorney, I also investigated and prosecuted bank fraud and other offenses.

3. Based on your affiant's training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Kyle STEVENS ("STEVENS") has committed violations of 18 U.S.C. §§ 875(c) (threats made in interstate or foreign commerce), 2261A(2) (cyberstalking), 641 (theft concerning programs receiving federal funds), 1343 (wire fraud) and 1957 (money laundering), (the "TARGET OFFENSES"). There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is:

- Chromebook laptop (S/N: 7L0w242)
- Teclast laptop (S/N: 8353S212663404)
- Acer laptop (S/N: NXEFUEG00302108EA92N00)
- HP PC computer (S/N: 4CE1151FG7)
- PC Tower Erazer Mediom MT39 computer (S/N: 162207050900275)

- Dark blue Galaxy S6 cell phone
- Dark blue Samsung cell phone in a red and black case
- Dark blue Samsung cell phone with no case
- External hard drive

The nine electronic Devices are collectively referenced herein as the “Devices.” They are currently located in an evidence locker at the Federal Bureau of Investigation’s Wilmington Resident Agency, 500 Delaware Avenue, Wilmington, Delaware 19801.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

CASE BACKGROUND

6. During the 2018-2019 school year, STEVENS was a student at the University of Delaware. He met two female students, Victims 1 and 2, and, over the course of months, sent them text messages saying things like “I hate you [Victim 1]” and “Yo [Victim 2], I hope you go to hell you trashy, spoiled scumbag.” The University of Delaware Police Department and Newark Police Department opened an investigation into STEVENS and, on December 11, 2019, STEVENS was arrested and charged with stalking and harassment in violation of state law. He pled guilty to harassment concerning Victim 1 and was placed on probation.

7. While on probation, STEVENS applied and was accepted to the University of Freiburg, located in Freiburg, Germany. STEVENS’s probation was terminated early so he could attend the University of Freiburg. On or about October 29, 2020, STEVENS left the United States to attend college in Germany.

8. Approximately two weeks after STEVENS moved to Germany, in November 2020, he resumed contacting Victim 1 via email, and continued contacting her ultimately through August 2022 via multiple email accounts and social media platforms. In September and October

2021, STEVENS resumed contacting Victim 2, via Venmo, a cell phone application. The messages, further described below, repeatedly referenced STEVENS hating and wanting to harm Victims 1 and 2.

9. As a result of STEVENS' messages to Victims 1 and 2 while abroad, the FBI opened an investigation into STEVENS for cyberstalking and sending threatening communications in foreign commerce. Over the course of that investigation, the FBI obtained warrants to search STEVENS' email accounts (Case Nos. 21-311M, 21-312M, 21-313M, signed by United States Magistrate Judge Sherry R. Fallon on November 12, 2021) and Facebook accounts (Case No. 22-265M, signed by then-Chief United States Magistrate Judge Mary Pat Thyng on August 22, 2022).

10. The FBI also discovered that, in 2021, STEVENS submitted ten fraudulent applications to the U.S. Small Business Administration (the "SBA") and/or its authorized lenders in order to obtain loans through small business loan programs established by the passing of The Coronavirus Aid, Relief, and Economic Security Act, also known as the CARES Act. Six of those loans were funded for a total of \$1,428,664.14, through the SBA programs targeted at relief for small businesses. The applications were made on behalf of five entities which STEVENS purported to own and control. Each of the loan applications falsely claimed that STEVENS' businesses had a number of employees, gross revenues, and were in operation at the start of the Coronavirus Pandemic. In fact, the businesses did not exist.

11. On July 14, 2022, a federal grand jury sitting in the District of Delaware returned two Indictments charging STEVENS with two counts of stalking, in violation of 18 U.S.C. § 2261A(2), and five counts of threats in foreign commerce, in violation of 18 U.S.C. § 875(c) (Indictment 22-65) as well as ten counts of wire fraud, in violation of 18 U.S.C. § 1343 and

seven counts of money laundering, in violation of 18 U.S.C. § 1957 (Indictment 22-66). An arrest warrant was issued for STEVENS on July 15, 2022.

12. On October 12, 2022, the government issued a request to Germany to extradite STEVENS to the United States to stand trial on the two Indictments. The United States also requested, pursuant to the United States-Germany Mutual Leal Assistance Treaty (MLAT), that at the time of STEVENS' arrest for extradition, German law enforcement seize electronic devices found on STEVENS' person, in any bags near his person, in his home, or in his vehicle in a manner consistent with German law.

13. On March 15, 2023, German authorities arrested STEVENS and seized his electronic devices pursuant to the MLAT (the Devices). Since that time, the electronic devices have been secured in German law enforcement custody and STEVENS has completed extradition proceedings in the German court system.

14. On May 10, 2023, the government received notice that Germany completed its extradition proceedings and had formally granted the request for STEVENS' extradition. On May 23, 2023, Your Affiant and other law enforcement personnel travelled to Germany to take STEVENS into custody and retrieve the Devices. Your Affiant returned to Delaware with STEVENS and the Devices on May 25, 2023. The Devices are currently in an evidence locker at the FBI's Wilmington Resident Agency. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this

investigation, in substantially the same state as they were when the Devices first came into the possession of the FBI.

PROBABLE CAUSE

Cyberstalking and True Threats

15. Your Affiant has probable cause to believe that the Devices will contain evidence of cyberstalking and true threats. Each of the devices has the ability to access the internet, to store data from the internet, and/or to send communications to a person's cellular telephone. As described further below, STEVENS sent Victims 1 and 2 threatening communications through multiple platforms, and the devices are likely to contain evidence of those communications, including the communications themselves and/or evidence that STEVENS owned and accessed the email and social media accounts and telephone numbers used to send those messages.

16. STEVENS sent Victims 1 and 2 numerous threatening messages through a variety of email addresses and social media platforms. For example, on November 14, 2020, Victim 1 received the following email from kyleastevens@gmail.com:

From:¹ Kyle Anthony Stevens [kyleastevens@gmail.com]
Subject: you just couldn't be honest
Body: And you'll never be. Now we'll have this problem forever. Hopefully I don't lose my mind when I run into you again.

The email account used to send that message, kyleastevens@gmail.com, is the same account STEVENS provided to the University of Delaware when he applied for admission. In addition, subpoenaed information from Google indicates that the account is subscribed to "Kyle Anthony

¹ Your affiant is aware that user-inputted names, here "Kyle Anthony Stevens" are often automatically populated in email messages in front of the email address sending the message.

Stevens” and is connected to the telephone number 609-579-0445, the same telephone number STEVENS provided to the University of Delaware when he applied for admission.

17. On September 12, 2021, Victim 1 received a text message from +49-151-24011594. Your affiant conducted open-source research and determined that +49 is the area code for Germany, where STEVENS was living at the time. The message stated:

Why couldn’t you just be honest?

18. On October 24, 2021 Victim 1 received the following email from kyleastevens@gmail.com:

Subject: I’m going to kill you.

Body: Tell everyone. You’re dead. All because you couldn’t be honest for even a minute.

19. On October 28, 2021, Victim 2 received two Venmo requests for \$0.01 each from an individual with the username @kyle-stevens-185, with the display name “Kyle Stevens.” The messages associated with the requests stated the following:

For the bullet I’m going to put in your head. Worthless lying, shady Jew sack of shit

Bet you won’t be able to block a gunshot.

According to subpoenaed records from Venmo, the Venmo account used to send that message is connected to the email address kanthonystevens@gmail.com. According to subpoenaed records from Google, kanthonystevens@gmail.com is subscribed to K. Anthony Stevens and is linked to the recovery email address kyleastevens@gmail.com (discussed above).

20. On March 8, 2022, Victim 1 received a message from a Facebook account with ID number 100028593182427 stating: “Can’t wait to send a bullet crashing through your skull.” That Facebook account is in the name of “Kyle Stevens” and has a profile picture that is

consistent with the appearance of STEVENS. The account was registered using the email address kyleastevens@buccaneer.atlantic.edu, a domain associated with Atlantic Cape Community College, where STEVENS was previously enrolled. Atlantic Cape Community College records confirm that this was the email address associated with STEVENS while he attended the college.

21. The above messages are a representative sample, but not all, of the messages STEVENS sent to Victims 1 and 2 via various platforms while living in Germany. The Devices are capable of sending and/or storing electronic communications. Your Affiant believes, based on training and experience, that electronic communications like emails, Facebook messages, Venmo messages, and text messages, do not automatically delete, and that criminals often save evidence of their crimes in places they believe are private. A further description of the ability of electronic devices to store data for long periods of time appears below under the heading “Electronic Storage and Forensic Analysis.”

CARES Act Fraud

STEVENS Applies for Ten Fraudulent CARES Act Loans or Grants

22. Your Affiant also has probable cause to believe that the Devices will contain evidence of wire fraud and money laundering. As described further below, from January 26, 2021 to December 26, 2021, STEVENS applied for multiple small business loans or grants through the Coronavirus Aid, Relief, and Economic Security Act (“CARES Act”), which provided loans or grants to small businesses negatively impacted by the pandemic. Five of STEVENS’ applications were granted, and STEVENS received \$1,428,664.14 in fraudulently obtained funds, which he transferred to various bank and investment accounts. Because STEVENS submitted each of his applications through the internet, and because his bank and

investment accounts are accessible online, there is probable cause to believe that the Devices, which can access the internet and/or save data from the internet, will contain evidence of STEVENS' wire fraud and money laundering.

23. STEVENS submitted his first application on January 26, 2021, to Cross River Bank. The application was in the name of Stevens Contracting, a business purportedly located in Hamilton, New Jersey. It was submitted online using the email address stevenscontracting17@gmail.com. The FBI determined that STEVENS submitted the application because a subpoena to Google revealed that the email account is connected to a Google Pay account linked to a Visa debit card associated with a Wells Fargo bank account ending 2810 (the WF 2810 Account). A subpoena to Wells Fargo revealed that STEVENS opened the WF 2810 Account and is the sole signer on the account. The FBI determined that the loan application was fraudulent because the business address STEVENS provided for Stevens Contracting is his mother's home address. In addition, there is no internet presence for a Stevens Contracting business located in New Jersey. Further, STEVENS' bank accounts lacked any expenses or revenues consistent with running a construction business. The application was approved and \$240,416 was deposited into the WF 2810 Account.

24. STEVENS submitted his second application on March 22, 2021, to Cross River Bank. The application was also in the name of Stevens Contracting, and was also submitted using the email address stevenscontracting17@gmail.com. The FBI determined that the application was fraudulent because of the lack of internet presence for a Stevens Contracting business in New Jersey and because of the lack of banking activity consistent with running a construction business. The application was denied.

25. STEVENS submitted his third application on March 22, 2021, to Lendio, a lender approved by the Small Business Administration (SBA) to disburse funds under the CARES act. The application was also in the name of Stevens Contracting. It was submitted using the email address kanthonystevens@gmail.com, which has been linked to STEVENS as discussed in paragraph 19 above. The FBI determined that the application was fraudulent because of the lack of internet presence for a Stevens Contracting business in New Jersey and because of the lack of banking activity consistent with running a construction business. In addition, STEVENS submitted different details for Stevens Contracting across his applications for that purported business, including different numbers of employees, entity start dates, and monthly payroll. The application was denied.

26. STEVENS submitted his fourth application on April 6, 2021, to the SBA. The application was submitted in the name of Kyle Stevens with the trade name Stevens Contracting. The application listed the email address stevenscontracting17@gmail.com. The FBI determined that the application was fraudulent because, as set forth above, there is no indicia on the internet or in STEVENS' bank records that Stevens Contracting is a legitimate business. The application was denied.

27. STEVENS submitted his fifth application on March 23, 2021, to Customers Bank. The application was in the name of Kyle Stevens as a sole proprietorship. The application listed the email address stevenscontracting17@gmail.com. The FBI determined that the application was fraudulent because it listed his mother's home address as his business address and stated he had \$44,950 in monthly payroll expenses, while his bank account activity showed no indicia of payroll expenses or other expenses consistent with running a business. The application was granted, and \$112,375 was deposited into STEVENS' WF 2810 Account.

28. STEVENS submitted his sixth application on April 24, 2021, to ReadyCap Lending. The application was in the name of Stevens Contracting. The application listed the email address stevenscontracting17@gmail.com. The FBI determined that the application was fraudulent because, as set forth above, there is no indicia on the internet or in STEVENS' bank records that Stevens Contracting is a legitimate business. The application was granted, and \$359,567 was deposited into STEVENS' WF 2810 Account.

29. STEVENS submitted his seventh application on August 21, 2021, to the SBA. The loan was in the name of the Artisan Theater in Northfield, New Jersey. The application was submitted using the email address artisantheater@gmail.com. The FBI determined that STEVENS submitted the loan application because subpoenaed records from Google revealed that the email account is connected to stevenscontracting17@gmail.com. The FBI determined that the application was fraudulent because there is no internet presence for an Artisan Theater in New Jersey and STEVENS' bank account activity showed no indicia of payroll expenses or other expenses consistent with running a business. In addition, as further described in paragraph 30 below, a future application for the Artisan Theater revealed that STEVENS submitted a falsified internet search result for the Artisan Theater. The application was granted, and \$447,536.76 was deposited into STEVENS' WF 2810 Account.

30. STEVENS submitted his eighth application on September 15, 2021, to the SBA. The loan was in the name of the Artisan Theater in Northfield, New Jersey. The application was submitted using the email address stevenscontracting17@gmail.com. The FBI determined that the application was fraudulent because the street address STEVENS provided for the Artisan Theater in New Jersey is the address of a different business, the Tilton Theater. An internet search revealed that STEVENS submitted a picture of the Google search result for the Tilton

Theater with his loan application but manipulated the picture to appear as if it was a Google search result for a business called the Artisan Theater. In addition, STEVENS' bank account activity showed no indicia of revenue or expenses consistent with running a theater. The application was denied.

31. STEVENS submitted his ninth application, a request for additional funds associated with his August 21, 2021 application for the Artisan Theater, on October 22, 2021. As with the August 21, 2021 application and the September 15, 2021 application, the FBI determined that this application was fraudulent because there is no indicia that the Artisan Theater exists or that STEVENS' bank accounts have revenue or expenses consistent with running a theater. The request for additional funding was granted and \$238,768 was deposited into STEVENS' WF 2810 Account.

32. STEVENS submitted his tenth application on December 26, 2021, to the SBA. The application was in the name of Kyle Stevens as a sole proprietorship doing construction and contracting work. The application was submitted using the email address kyleastevens@gmail.com, which has been linked to STEVENS as described in paragraph 16 above. The FBI determined that the application was fraudulent because it listed his mother's home address as his business address and stated he had \$1,061,193 in annual gross revenues, while his bank account activity showed no indicia of revenues or expenses consistent with running a business. The application was denied.

33. The FBI discovered further indicia of fraud when comparing STEVENS' applications to each other. For example, Stevens submitted the same check in support of his March 22, 2021 application for the Cross River Loan on behalf of Stevens Contracting and his unsuccessful September 15, 2021 application on behalf of the Artisan Theater. The checks have

the same check number, 0293, from the same bank, Wells Fargo, and were altered only to reflect different business names in the upper left corner of the check. Images of the two checks are below.

Kyle A Stevens, Stevens Contracting
34 Meadow Cir
Mays Landing, NJ 08330

0293

Date May 14, 2020

Pay to the
Order of _____

VOID

\$ _____

Dollars



Wells Fargo Bank N.A.
6010 Main St
Mays Landing, NJ 08330

Memo _____



Kyle A Stevens, The Artisan Theater
34 Meadow Cir
Mays Landing, NJ 08330

0293


Date May 14, 2020

Pay to the
Order of _____


VOID

\$ _____

Dollars

 **Wells Fargo Bank N.A.**
6010 Main St
Mays Landing, NJ 08330

Memo _____



34. In addition, Stevens submitted the same payroll register with the August 21, 2021 application for the Artisan Theater and with the April 24, 2021 application for the ReadyCap Loan on behalf of Stevens Contracting. Both payroll registers list the same nineteen employees, including four who share Stevens' last name, and Mansour Farbod, Stevens' father. Images of the two ledgers are below.

The Artisan Theater
331 Tilton Road
Northfield, NJ 08225

February 2020 Payroll Register
Prepared by: Kyle Stevens

Employee ID	Name	Hourly Wage	Hours	Gross Pay	State Unemployment 7%	Social Security 6.2%	Medicare 1.45%	Total Tax Withheld (Excluding Federal Income)	Net Pay (Excluding Federal Income)
1	Stevens, Manny	\$30.50	90	\$2745.00	\$192.15	\$170.19	\$39.80	\$402.14	\$2342.86
2	Stevens, James	\$25.00	122	\$3050.00	\$213.50	\$189.10	\$44.23	\$446.83	\$2603.18
3	Stevens, Kyle	\$30.50	169	\$5154.50	\$360.82	\$319.58	\$74.74	\$755.13	\$4399.67
5	Stevens, Casey	\$26.00	180	\$4680.00	\$327.60	\$290.16	\$67.86	\$685.62	\$3994.38
6	Stevens, Joe	\$20.00	167	\$3340.00	\$233.80	\$207.08	\$48.43	\$489.31	\$2850.69
7	Kearney, Liam	\$22.00	125.5	\$2761.00	\$193.27	\$171.18	\$40.03	\$404.49	\$2356.51
8	Kane, Mark	\$17.00	133	\$2261.00	\$158.27	\$140.18	\$32.78	\$331.24	\$1929.76
9	Willson, Andrew	\$18.50	138	\$2553.00	\$178.71	\$158.29	\$37.01	\$374.01	\$2178.98
10	Calloway, Paul	\$12.00	158	\$1896.00	\$132.72	\$117.55	\$27.49	\$277.76	\$1618.24
11	Muhammed, Sandeep	\$15.00	160	\$2400.00	\$168.00	\$148.80	\$34.80	\$351.60	\$2048.40
14	Braun, Dieter	\$12.00	122	\$1464.00	\$102.48	\$90.77	\$21.23	\$241.48	\$1249.52
17	Stevens, Will	\$12.00	120	\$1440.00	\$100.80	\$89.28	\$20.88	\$210.96	\$1229.04
19	Heckman, Justin	\$12.00	140	\$1680.00	\$117.60	\$104.16	\$24.36	\$246.12	\$1433.88
22	Septeoe, Lori	\$12.00	160	\$1920.00	\$134.40	\$119.04	\$27.84	\$281.28	\$1638.72
23	Farbod, Mansour	\$13.00	100	\$1300.00	\$91.00	\$80.60	\$18.85	\$190.45	\$1109.55
25	Milov, Igor	\$12.50	50	\$625.00	\$43.75	\$38.75	\$9.06	\$91.56	\$533.44
30	Kawai, Masato	\$13.00	45	\$585.00	\$40.95	\$36.27	\$8.48	\$85.70	\$499.30
31	Griffin, Seth	\$12.00	65	\$780.00	\$54.60	\$48.36	\$11.31	\$114.27	\$665.73
36	Kane, John	\$12.00	80	\$960.00	\$67.20	\$59.52	\$13.92	\$140.64	\$819.36
				\$41,594.50	\$2,911.62	\$2,578.86	\$603.12	\$6,093.59	\$35,500.91

Stevens Contracting, Roofing and Gutter Construction and Repair
34 Meadow Circle
Mays Landing, NJ 08330

2019 Year-End Payroll Register
Prepared by: Kyle Stevens

Employee ID	Name	Hourly Wage	Hours	Gross Pay	State Unemployment 7%	Social Security 6.2%	Medicare 1.45%	Total Tax Withheld	Net Pay
1	Stevens, Manny	\$30.50	3042.00	\$92,781.00	\$6,494.67	\$5,752.42	\$1,391.72	\$13,638.81	\$79,142.19
2	Stevens, James	\$25.00	3519.00	\$87,975.00	\$6,158.25	\$5,454.45	\$1,319.63	\$12,932.33	\$75,042.68
3	Stevens, Kyle	\$40.50	2345.00	\$94,972.50	\$6,648.08	\$5,888.30	\$1,424.59	\$13,960.96	\$81,011.54
5	Stevens, Casey	\$36.00	2655.00	\$95,580.00	\$6,690.60	\$5,925.96	\$1,433.70	\$14,050.26	\$81,529.74
6	Stevens, Joe	\$30.00	3010.00	\$90,300.00	\$6,321.00	\$5,598.60	\$1,354.50	\$13,274.10	\$77,025.90
7	Kearney, Liam	\$22.00	3585.00	\$78,870.00	\$5,520.90	\$4,889.94	\$1,183.05	\$11,593.89	\$67,276.11
8	Kane, Mark	\$27.00	3001.00	\$81,027.00	\$5,671.89	\$5,023.67	\$1,215.41	\$11,910.97	\$69,116.03
9	Wilson, Andrew	\$25.50	2987.00	\$76,168.50	\$5,331.80	\$4,722.45	\$1,142.53	\$11,196.77	\$64,971.73
10	Calloway, Paul	\$31.00	2959.00	\$91,729.00	\$6,421.03	\$5,687.20	\$1,375.94	\$13,484.16	\$78,244.84
11	Muhammed, Sandeep	\$15.00	4985.00	\$74,775.00	\$5,234.25	\$4,636.05	\$1,121.63	\$10,991.93	\$63,783.08
14	Braun, Dieter	\$25.00	2868.00	\$71,700.00	\$5,019.00	\$4,445.40	\$1,075.50	\$10,539.90	\$61,160.10
17	Stevens, Will	\$25.00	3014.00	\$75,350.00	\$5,274.50	\$4,671.70	\$1,130.25	\$11,076.45	\$64,273.55
19	Heckman, Justin	\$25.25	3304.00	\$83,426.00	\$5,839.82	\$5,172.41	\$1,251.39	\$12,263.62	\$71,162.38
22	Septeoe, Lori	\$25.00	3894.00	\$97,350.00	\$6,814.50	\$6,035.70	\$1,460.25	\$14,310.45	\$83,039.55
23	Farbod, Mansour	\$31.00	2985.00	\$92,535.00	\$6,477.45	\$5,737.17	\$1,341.76	\$13,556.38	\$78,978.62
25	Milov, Igor	\$19.00	4950.00	\$94,050.00	\$6,583.50	\$5,831.10	\$1,363.73	\$13,778.33	\$80,271.68
30	Kawai, Masato	\$23.00	3545.00	\$81,535.00	\$5,707.45	\$5,055.17	\$1,182.26	\$11,944.88	\$69,590.12
31	Griffin, Seth	\$21.60	4539.00	\$98,042.40	\$6,862.97	\$6,078.63	\$1,421.61	\$14,363.21	\$83,679.19
36	Kane, John	\$23.00	2945.00	\$67,735.00	\$4,741.45	\$4,199.57	\$982.16	\$9,923.18	\$57,811.82
				1,625,901.40	113,813.098	100,805.8868	24,171.5723	238,790.5571	1,387,110.8429

STEVENS Transfers Fraudulently Obtained Funds to Multiple Bank and Investment Accounts

35. Once STEVENS received fraudulently obtained loan or grant funds, he transferred them among various bank accounts such as Schwab Brokerage, the Vanguard Group, and Fidelity Brokerage, as well as cryptocurrency and stock exchange companies such as Robinhood and Coinbase, Inc.

36. On July 30, 2020, STEVENS opened an account with Robinhood Markets, Inc. with account number [REDACTED] (the "Robinhood Account"). Through a grand jury subpoena,

Your Affiant learned that STEVENS opened the Robinhood Account using a Samsung Galaxy phone, STEVENS' New Jersey driver's license photo, email address kyleastevens@gmail.com, telephone number 609-579-0455, and his mother's home address.

37. On January 24, 2021, STEVENS opened account [REDACTED] with Transferwise. Through a grand jury subpoena, Your Affiant learned STEVENS also opened the account with STEVENS' New Jersey driver's license photo, email address kyleastevens@gmail.com and telephone number 609-579-0455. STEVENS provided an address in Freiburg Im Breisgau, Germany. Transferwise is an online international currency exchange. Between January and September 2021, STEVENS used Transferwise to exchange CARES Act funds into Euro, and deposit the funds into Sparkasse Account [REDACTED] held at Sparkasse Freiburg Bank in Germany ("the Sparkasse Account") and Volksbank Account [REDACTED] held at Volksbank Freiburg in Germany ("the Volksbank Account").

38. On May 10, 2021, STEVENS opened three investment accounts: the Schwab Account (# [REDACTED]), the Fidelity Account (# [REDACTED]), and the Vanguard Account (# [REDACTED]). Through grand jury subpoenas, Your Affiant learned all three accounts were opened by STEVENS, listing his mother's home address, email address kyleastevens@gmail.com, and STEVENS' date of birth. In the Schwab Account opening documents, STEVENS listed his employment status as "Student," and indicated the "Source of funds" was "family/relatives/inheritances; gifts." The Fidelity Account indicated that STEVENS was self-employed as a tennis instructor. The Vanguard Account also indicated STEVENS was self-employed as a tennis instructor, and listed the sources of money in the account as salary, social security benefits, investment gains, gift/inheritance, and working capital.

39. Your Affiant reviewed bank records from the WF 2810 Account and a savings account at Wells Fargo which STEVENS opened and for which STEVENS is the sole signer (the “WF 5270 Account”). Your Affiant also reviewed records for the Robinhood Account, the Schwab Account, the Fidelity Account, the Vanguard Account, and for STEVENS’ Transferwise account. Tracing for each loan was completed using a proceeds-out-first method. Under this method, when commingled funds are in an account, criminal proceeds are withdrawn first, leaving the legitimate funds in the account. When there are insufficient proceeds to cover a specific withdrawal, then legitimate funds are used to cover the withdrawal.

40. On February 23, 2021, the Cross River Loan of \$240,416 was deposited into the WF 2810 Account. Following this deposit, STEVENS made, among others, the following transfers of funds,² each of which, based on the tracing performed, contained over \$10,000 of fraudulently obtained funds:

- a. On or about February 25, 2021, \$50,000 from the WF 2810 Account to the Robinhood Account;
- b. On or about February 25, 2021, \$20,000 from the WF 2810 Account to the Sparkasse Account, via Transferwise;
- c. On or about March 3, 2021, \$50,000 from the WF 2810 Account to the Robinhood Account;
- d. On or about March 11, 2021, \$20,000 from the WF 2810 Account to the Sparkasse Account;

² Your Affiant is aware of the exact amount transferred to each account. When the numbers are not round, approximate figures are used to facilitate calculations in this affidavit.

- e. On or about March 11, 2021, \$50,000 from the WF 2810 Account to the Robinhood Account;
 - f. On or about April 5, 2021, \$50,000 from the Robinhood Account to the WF 2810 Account;
 - g. On or about April 5, 2021, \$10,000 from the WF 2810 Account to the Volksbank Account, via Transferwise;
 - h. On or about April 6, 2021, \$10,000 from the WF 2810 Account to the Volksbank Account, via Transferwise;
 - i. On or about April 6, 2021, \$50,000 from the Robinhood Account to the WF 2810 Account; and
 - j. On or about April 7, 2021, \$50,000 from the Robinhood Account to the WF 2810 Account.
41. Your Affiant determined that the proceeds of the Cross River Loan were transferred as follows from on or about February 24, 2021 through on or about April 8, 2021:
- a. \$2,000 to the Robinhood Account
 - b. \$80,000 converted via Transferwise to approximately €65,700 sent to the Sparkasse Account; and
 - c. Approximately \$24,500, converted via Transferwise to approximately €20,600 sent to the Volksbank Account.
42. On April 9, 2021, the Customers Loan of \$112,375 was deposited into the WF 2810 Account. At this time, the WF 2810 Account still held over \$100,000 of proceeds traceable to the Cross River Loan. Following this deposit, STEVENS made, among others, the following transfers

of funds, each of which, based on the tracing performed, contained over \$10,000 of fraudulently obtained funds:

- a. On or about April 19, 2021, \$20,000 from the WF 2810 Account to the Sparkasse Account, via Transferwise;
- b. On or about April 30, 2021, \$200,000 from the WF 2810 Account to the WF 5270 Account; and
- c. On or about May 12, 2021, \$190,000 from the WF 5270 Account to the Fidelity Account.

43. Your Affiant determined that the remaining proceeds of the Cross River Loan and Customers Loan were transferred as follows from on or about April 19, 2021 through on or about May 12, 2021:

- a. \$20,000, converted via Transferwise to approximately €16,500, sent to the Sparkasse account; and
- b. \$190,000 to the Fidelity Account.³

44. On May 5, 2021, the Readycap Loan of \$359,568 was deposited into the WF 2810 Account. Prior to deposit of the Readycap Lending loan, the WF 2810 Account held over \$24,000 of proceeds traceable to prior fraudulent loans. Following this deposit, STEVENS made, among others, the following transfers of funds, each of which, based on the tracing performed, contained over \$10,000 of fraudulently obtained funds:

³ On or about April 30, 2021, Stevens transferred \$200,000 of proceeds from the Cross River Loan and the Customers Loan from the WF 2810 Account to the WF 5270 Account. From the WF 5270 Account the proceeds were then transferred to the Fidelity Account.

- a. On or about May 12, 2021, \$100,000 from the WF 2810 Account to the Schwab Account;
- b. On or about May 12, 2021, \$30,000 from the WF 2810 Account to the Schwab Account;
- c. On or about May 14, 2021, \$100,000 from the WF 2810 Account to the Schwab Account; and
- d. On or about May 14, 2021, \$150,000 from the WF 2810 Account to the Fidelity Account.

45. Your Affiant determined that from on or about May 12, 2021 through on or about July 21, 2021, the proceeds from the Readycap Loan and remaining proceeds traceable to prior fraudulent loans were transferred as follows:

- a. \$200,000 to the Schwab Account;
- b. \$150,000 to the Fidelity Account; and
- c. Approximately \$33,000 to the Vanguard Account.

46. On October 15, 2021, the First Artisan Theater SBA Grant of \$477,536.76 was deposited into the WF 2810 Account. Following this deposit, STEVENS made, among others, the following transfers of funds, each of which, based on the tracing performed, contained over \$10,000 of fraudulently obtained funds:

- a. On or about October 25, 2021, \$470,000 from the WF 2810 Account to the WF 5270 Account;
- b. On or about October 25, 2021, \$120,000 from the WF 5270 Account to the WF 2810 Account;

- c. On or about October 27, 2021, \$100,000 from the WF 5270 Account to the Schwab Account;
- d. On or about October 27, 2021, \$250,000 from the WF 5270 Account to the Fidelity Account;
- e. On or about October 27, 2021, \$120,000 from the WF 2810 Account to the Vanguard Account;
- f. On or about November 3, 2021, \$99,321.22 from the Vanguard Account to the WF 2810 Account; and
- g. On or about November 9, 2021, \$100,000 from the WF 2810 Account to the Fidelity Account.

47. Your Affiant determined that, from on or about October 27, 2021, through on or about November 9, 2021, the proceeds from the First Artisan Theater Grant were transferred as follows:

- a. \$100,000 to the Schwab Account;
- b. \$350,000 to the Fidelity Account; and
- c. Approximately \$20,700 to the Vanguard Account.

48. On November 15, 2021, the Second Artisan Theater SBA Grant for \$238,768.38 was deposited into the WF 2810 Account. Prior to deposit of the second grant, over \$2,000 of proceeds from the First Artisan Theater Grant remained in the WF 2810 Account. Following this deposit, STEVENS made, among others, the following transfers of funds, each of which, based on the tracing performed, contained over \$10,000 of fraudulently obtained funds:

- a. On or about November 19, 2021, \$190,000 from the WF 2810 Account to the Fidelity Account; and

- b. On or about November 19, 2021, \$50,000 from the WF 2810 Account to the Robinhood Account.

49. Your Affiant determined that on or about November 19, 2021, the remaining proceeds from the First Artisan Theater Grant and proceeds from the Second Artisan Theater Grant were transferred as follows:

- a. \$190,000 to the Fidelity Account; and
- b. \$50,000 to the Robinhood Account.

50. In total, between on or about July 14, 2021 and on or about November 10, 2021, proceeds from the fraudulently obtained loans and grants were transferred as follows:

- a. \$880,000 to the Fidelity Account;
- b. \$300,000 to the Schwab Account;
- c. Approximately \$108,000 to the Robinhood Account;
- d. \$115,000, converted to approximately €94,500 to the Sparkasse Account;
- e. Approximately \$53,700 to the Vanguard Account;
- f. Approximately \$24,500, converted to approximately €20,600, to the Volksbank Account.

STEVENS Utilized the DEVICES to Prepare and Submit Fraudulent Loan Applications, Supporting Documents, and Investment Account Applications

51. As described above, STEVENS submitted ten fraudulent loan applications between January and December 2021. After receiving the loan proceeds, STEVENS transferred the funds to investment accounts opened at Schwab, Fidelity, Vanguard, Robinhood, as well as conducted transfers to German accounts via Transferwise. Your affiant reviewed the loan applications, corresponding supporting documents, and financial account documentation. Based

on a review of the loan and financial account documentation, Your affiant determined STEVENS utilized personal electronic devices to prepare the fraudulent loan documents and open the investment accounts. For example, when opening his Schwab investment account, as well as both Cross River Bank loan applications, STEVENS used Mozilla/5.0, a free and publicly available internet web browser accessible via mobile application and other personal electronic devices. STEVENS also used cellular applications including Schwab Mobile for Android, a cellular telephone application developed for managing Schwab investment accounts and transactions, and Transferwise, a digital bank accessible via mobile application and web browser. Additionally, Your affiant is aware STEVENS accessed his Robinhood account via a Galaxy A 71 5G Samsung SM A 716 V cellular telephone.

52. STEVENS also used web-based customer assistance software to complete the loan applications. For example, STEVENS' Readycap Lending loan application was completed, in part, using Docusign⁴ and Salesforce⁵ software. STEVENS also created the fictitious business domain artisantheaternj.com via GoDaddy, a web-based domain registrar. In my training and experience, I am aware that electronic devices which access web-based software often maintain records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

⁴ Docusign is a document signing software utilized for creating secure electronic signautres.

⁵ American cloud-based software company providing a customer relationship, sales, and operation management platform.

53. Additionally, as described in further detail above, Your affiant determined STEVENS used computer software to prepare fraudulent loan application supporting documents, including- fictitious payroll records, tax forms, images of voided checks, and screenshots of fictitious Google search pages. Based on Your affiant's training and experience, I am aware files maintained on personal electronic devices do not automatically delete, and that criminals often save evidence of their crimes in places they believe are private.

54. Your Affiant has probable cause to believe that evidence of STEVENS' fraudulent loan and grant applications, and his receipt and transfer of those proceeds, will be found on the DEVICES. The loan and grant applications were submitted online and connected with STEVENS' email addresses. Proceeds were deposited into STEVENS' bank account and then transferred to other bank and investment accounts which are accessible online. There is probable cause to believe evidence that STEVENS created and submitted the applications, controls the email accounts used to do so, and accessed the bank and investment accounts will be found on the DEVICES. In addition, there is probable cause to believe that such data has not been deleted over time. Your Affiant knows, from training and experience, that it is common for people to save financial information and documentation for long periods of time, and that internet search histories including records of logging into bank accounts are not automatically deleted. A further description of the ability of electronic devices to store data for long periods of time appears below under the heading "Electronic Storage and Forensic Analysis."

TECHNICAL TERMS

55. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless Devices used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the Devices.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images.

This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- d. Internet: The Internet is a global network of computers and other electronic Devices that communicate with each other. Due to the structure of the Internet, connections between Devices on the Internet often cross state and international borders, even when the Devices communicating with each other are in the same state.

56. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone and digital camera and to access the internet, and/or to store such electronic data. In my training and experience, examining data stored on Devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

57. Based on my knowledge, training, and experience, I know that electronic Devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the Devices. This information can sometimes be recovered with forensics tools.

58. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- e. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- f. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- g. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- h. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

59. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- i. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage Devices or other external storage media, and the times the computer was in use. Computer file

systems can record information about the dates files were created and the sequence in which they were created.

- j. Forensic evidence on a Device can also indicate who has used or controlled the Device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- k. A person with appropriate familiarity with how an electronic Device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic Devices were used, the purpose of their use, who used them, and when.
- l. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- m. Further, in finding evidence of how a Device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- n. I know that when an individual uses an electronic Device to contact a victim, submit a fraudulent document, or transfer fraudulent proceeds, the individual’s electronic Devices will generally serve both as an instrumentality for committing

the crime, and also as a storage medium for evidence of the crime. The electronic Devices are an instrumentality of the crime because they were used as a means of committing the criminal offense. The electronic Devices are also likely to be a storage medium for evidence of crime. From my training and experience, I believe that electronic Devices used to commit a crime of this type may contain: data that is evidence of how the electronic Devices were used; data that was sent or received; and other records that indicate the nature of the offense.

60. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

61. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

62. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Katherine Martinez
Katherine Martinez
Special Agent
Federal Bureau of Investigation

Sworn to me over the telephone and signed by me pursuant to
Fed. R. Crim. P. 4.1 on this 5th day of June, 2023:



HONORABLE SHERRY R. FALLON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is:

- Chromebook laptop (S/N: 7L0w242)
- Teclast laptop (S/N: 8353S212663404)
- Acer laptop (S/N: NXEFUEG00302108EA92N00)
- HP PC computer (S/N: 4CE1151FG7)
- PC Tower Erazer Mediom MT39 computer (S/N: 162207050900275)
- Dark blue Galaxy S6 cell phone
- Dark blue Samsung cell phone in red and black case
- Dark blue Samsung cell phone with no case
- External hard drive

Hereinafter the “Devices.” The Devices are currently located in an evidence locker at the Federal Bureau of Investigation’s Wilmington Resident Office, 500 Delaware Avenue, Wilmington, Delaware 19801.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. §§ 875(c) (threats made in interstate or foreign commerce), 2261A(2) (cyberstalking), 641 (theft concerning programs receiving federal funds), 1343 (wire fraud) and 1957 (money laundering), (the “TARGET OFFENSES”) and involve Kyle Stevens from January 1, 2021 including:

- a. Indicia of ownership and/or access to email accounts, social media platforms, telephone numbers, or other methods of communication;
- b. Any information related to victims of cyberstalking or threats;
- c. Indicia of ownership and/or access to financial accounts;
- d. All bank records, checks, credit card bills, account information, and other financial records;
- e. Any information related to loan or grant applications;
- f. Any information related to STEVENS’ businesses or other revenue streams, real or fictitious;
- g. Any information recording STEVENS’ schedule or travel from January 1, 2021 to the present;

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of Internet Protocol addresses including:

- a. records of Internet Protocol addresses used;

- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
District of Delaware

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*a Chromebook laptop (S/N: 7L0w242); Teclast laptop (S/N: a Chromebook laptop (S/N:
7L0w242); Teclast laptop (S/N: 8353S212663404); Acer laptop (S/N:
NXEFUEG00302108EA92N00); HP PC computer (S/N: 4CE1151FG7); PC Tower Eraser
Mediom MT39 computer (S/N: 162207050900275); Dark blue Galaxy S6 cell phone; Dark
blue Samsung cell phone in red/black case; Dark blue Samsung cell phone with no case;
and External hard drive

Case No. 23-252M

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

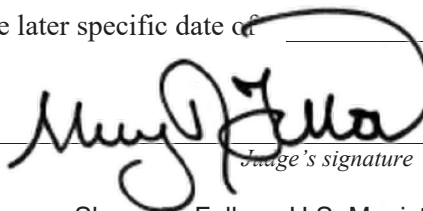
To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure
of the following person or property located in the _____ District of _____ Delaware*(identify the person or describe the property to be searched and give its location):*

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal *(identify the person or describe the property to be seized):*

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before June 19, 2023 *(not to exceed 14 days)*☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to _____ the duty U.S. magistrate judge
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized *(check the appropriate box)*☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.Date and time issued: 06/05/2023 2:36 p.m.City and state: Wilmington, DESherry R. Fallon, U.S. Magistrate Judge
Printed name and title

Return

Case No.:

23-

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title